



SECURITY GUIDE



Security User's Guide

A guide to using Project.net Security

Version 3.0

February 19, 2003

TABLE OF CONTENTS

Introduction	4
Roles	4
<i>Space Administrator</i>	4
<i>Team Member</i>	5
<i>Individual vs. Role-based Permissions</i>	5
Module Permissions	5
New Object Permissions	6
<i>Changes to New Object Permissions are not Retroactive</i>	7
Security can be modified three ways	7
Space Administrator – Setting Security	8
Navigate to the Security Manager	8
Setting Permissions for a Role or Person	9
<i>NOTE: Changes to Project.net Permissions</i>	Error! Bookmark not defined.
<i>Example of Module permissions overriding Object permissions</i>	12
Permissions Active - deactivate all permissions simultaneously	13
<i>To Simultaneously Deactivate all Permissions</i>	13
New Object Settings are not Retroactive!	13
<i>Deactivate a Person's Module Permissions</i>	15
<i>Deactivate a Role's Module Permissions</i>	15
<i>Deactivate a Person's New Object Permissions</i>	15
Discussion Forums – no security settings apply	16
Review: The Difference between Module and New Object Permissions	16
Hierarchy for the Permissions Active check box	16
Description of Modules and Objects	17
Team Members – Setting Security	19



SECURITY GUIDE

Setting Object Permissions	19
<i>Example: setting object permissions for a document</i>	<i>19</i>

Introduction

Only registered and licensed users can access the Project.net application by logging in. Only people that have been added (invited) to the team directory of a workspace are allowed to enter that space and access the information stored there.

Within each workspace, the **Space Administrator** can to set general access permissions (**Module Permissions**) for each module. The Space Administrator can also set **New Object Permissions** for the various object types in the workspace. **New Object Permissions** determine the access rules that are applied to objects by default when objects are created by a user. Individual **Object Permissions** can be changed by the person who created the object or by the Space Administrator after the object has been created.

The Project.net application offers several types of security:

- **password-based** authentication (login)
- **role-based** security settings
- **user-based** access controls on information
- **128-bit SSL encryption** between the client and server (optional)

Most Project.net users will only use the Security button  on the action toolbar to view and change **Object Permissions** on a specific object. By default, users can only view and change these permissions if they created the objects.

Each workspace has one or more “Space Administrators”. The Space Administrators are responsible for defining roles, adding people to roles and setting access permissions for the workspace. This is done from workspace directory module and the Setup link in the workspace.

Roles

SPACE ADMINISTRATOR

The Space Administrator is a special system-defined role in each workspace. The Space Administrator has full access to the entire workspace and controls permissions to all modules and objects within the workspace. The Space Administrator has the ability to control security and security permission throughout the workspace.

Security settings allow the space administrator to control which roles or individual team members can view, modify, create, or delete items in a project. The space administrator also controls who has the right to modify permissions for each module or object in the project, and can apply security at the **Module** level, as well as at the **New Object** level.

Before inviting users to a project, the Space Administrator should review and edit the Module Permissions and New Object Permissions for all roles in the project.

Recommendation: When setting up a new project, create roles (i.e., vendors, customers) and assign minimal permissions to the roles BEFORE inviting people to the project. This allows people to be assigned to their roles (and respective security settings) **at the same time** they are invited to the project. Change a role or individual's settings, as needed, to customize the security settings further. **(NOTE: All invitees are automatically assigned to the Team Member role.)**



SECURITY GUIDE

TEAM MEMBER

When **participants** (also known as “**users**” or “**team members**”) are initially invited to a Project.net project or business workspace, they automatically become members of the ‘Team Members’ role. All team members of a workspace are members of this role and cannot be removed from the Team Members role unless they are removed from the workspace. For this reason, it is important to **limit the permissions for the Team Member role**, especially if outside companies are involved in the project.

NOTE: Any team member who creates an object automatically has the right to modify all permissions for that object.

If you are not a Space Administrator, you can skip to **page 19** to learn how to set permissions for **individual objects**.

INDIVIDUAL VS. ROLE-BASED PERMISSIONS

The Space Administrator can apply access permissions to specific individuals as well as roles. Security is one of the most important reasons that Project.net team members should be divided into roles. These roles allow Space Administrators to easily set and change permissions for groups of people in one step.

Role-based permissions are additive. If a participant belongs to two roles, and one role has permission to view and modify a specific object, and the second role has permission only to view, then that participant will have permission to *both* view and modify.

Personal permissions override all Role-based permissions. If a person is granted permissions to a specific object (personal permission), all role-based permissions will be ignored for that user and object. For example, if the Team Member role allows *view*, *modify* and *delete* permissions to a specific document, but the user has a personal permission allowing only *view*, the user will not be able to modify or delete the document, only view it.

The personal permission is useful for granting extra permissions or removing permissions for a single user where creating a special group would be cumbersome. However, personal permissions are harder for the administrator to keep track of and manage. It is important to try to use role-based permissions instead of personal permissions whenever possible.

Module Permissions

Module permissions apply to an entire module such as Documents, Forms, Calendar, etc. They determine the Role or Person’s permission to access each module and access the objects within a module. If users do not have permission to view a module (through a role or personal permission), they will not be able to access that module or any of the items in that module. The following are the modules that permissions can be applied to:

SECURITY GUIDE

- Calendar
- Directory
- Discussion Forums
- Document Management
- Form Databases
- Workspace Templates
- News
- Project Process
- Project Schedule
- Project Space
- Security
- Workflow

NOTE: If participants create objects within a module and those participants later have *view* access revoked for that module, the participants will still be able to access the objects they created in that module. This is because team members are granted full access to any object that they have created.

New Object Permissions

New Object Permissions determine the default access permissions that will be assigned to each new object created within a workspace. It would be tedious for a user to manually apply permissions to every object that is created. The New Object Permissions allow the Space Administrator to set reasonable default permissions for each type of object in a workspace. A user can then change the permissions on a newly created object only if non-typical permissions are required. For example, the new object permissions should be setup so that the Customer role has view access to all documents and the Team Member role has view, modify, and remove permissions.

The following are objects that can be created and security can be applied to:

- Configuration Space
- Deliverable: A Phase Deliverable
- Discussion Group
- Document Folder
- Document
- Calendar Event
- Form Type
- Form instance data (all versions)
- Gate: A Phase Gate
- Security Group
- Calendar Meeting
- News
- Phase: A Process Phase
- Process: A Project Process
- Schedule Task or Milestone
- Workflow

CHANGES TO NEW OBJECT PERMISSIONS ARE NOT RETROACTIVE

Changes to New Object Permission settings do not affect previously created objects. Changes will only apply to new objects that are created in the future. So, if a team member adds a document to the Document Vault, and the space administrator later changes the New Object Permission for Documents, the team member's access to existing documents in the Document Vault will be unaffected. Items added prior to the changed in security must be secured individually by selecting the object, and then clicking the security  icon.

Definition of Actions

Permissions are composed of several Actions: view, modify, create, delete, and modify permission. These actions are generally defined as:

Module Permissions

View – The user can access a module and view the module's contents. The user access to module contents may be further limited by the object permissions on specific information within the module. If the user does not have view permission to the module, he will not be able to enter the module.

Modify -- The user has the ability to modify properties of a module (if any).

Create – The user has the ability to create new items within the module.

Delete – The user has the ability to delete items within the module. This permission may be overridden by specific object permissions.

Modify Permission – the user may modify the security permission for this module.

Object Permissions

View – The user can view (read-only) the object.

Modify -- The user has permission to modify the object.

Create – The user has permission to create new items of this object type.

Delete – The user has permission to delete the object.

Modify Permission – the user may modify the security permission for this object.

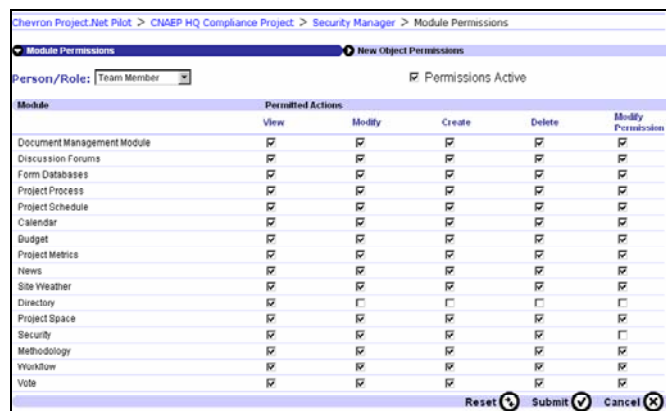
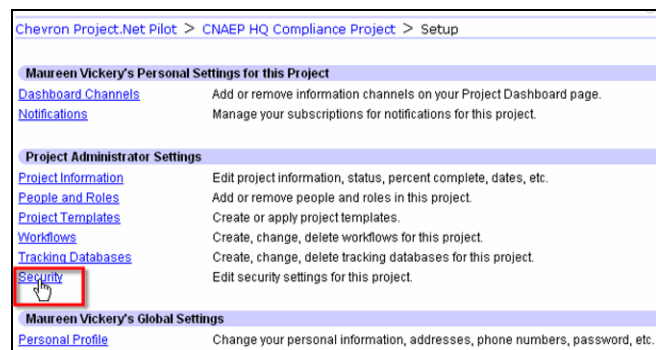
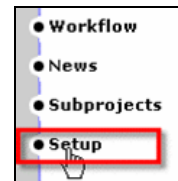
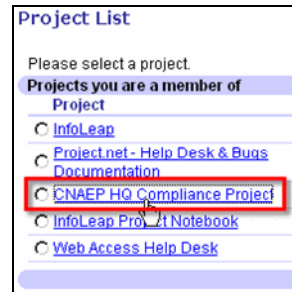
Security can be modified three ways

1. **Space Administrator** - Clicking **Setup** in the navigation bar to modify **Module** permissions.
2. **Space Administrator** - Clicking **Setup** in the navigation bar to modify **New Object** permissions.
3. **Space Administrator** or **Team Member** - Clicking the **Security**  button (when it is active) in the action toolbar to set permissions on **individual** objects such as forms or documents.

Space Administrator – Setting Security

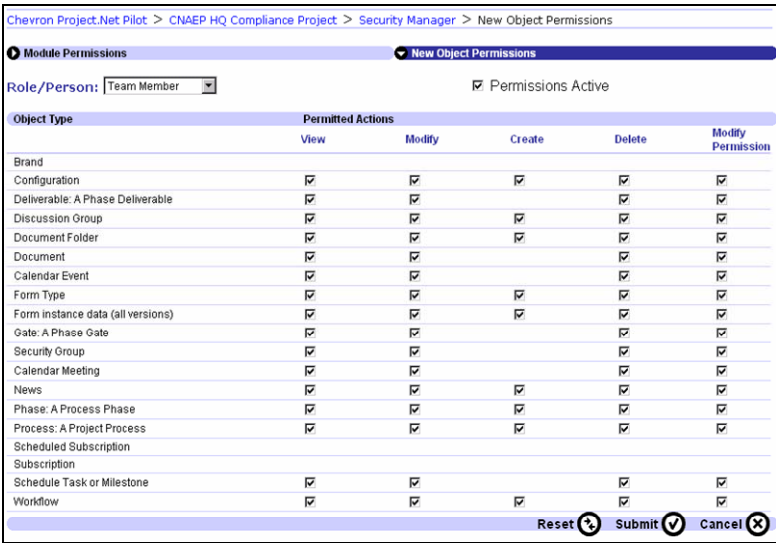
Navigate to the Security Manager

STEP	ACTION
1	Click the Projects button. The list of projects you are a member of appears in the Project Workspace.
2	Click the desired project. The project's Dashboard appears.
3	Click Setup in the left navigation bar. The Setup window appears.
4	Click Security under the Project Administrator Settings tab. The Security Manager window appears, defaulting to the Module Permissions tab. Notice that the permitted actions for each item are: - View - Modify - Create - Delete - Modify Permission



Continued on next page

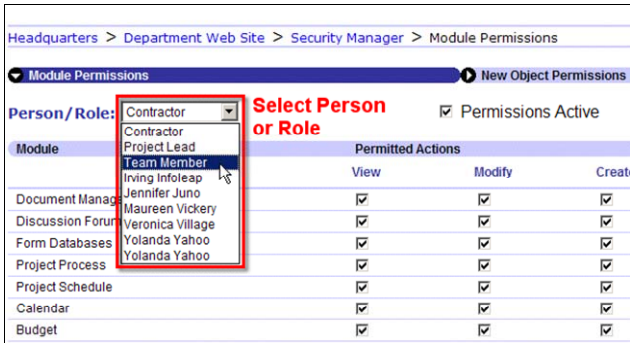
Navigate to the Security Manager (continued)

STEP	ACTION
5	Click the New Object Permissions tab. The New Object Permissions window appears.  

Setting Permissions for a Role or Person

For instructions on setting up roles, please see the **Project Setup** training module.

Security can be setup for roles or for individuals who are participants in a project. **NOTE:** A person's individual security settings will **override** any settings that the person has been assigned through the role(s) he/she belongs to.

STEP	ACTION
1	Navigate to the Security Manager window (page 8).
2	Select the role or person from the Person/Role drop-down list. In this example, we selected Team Member role. 

Continued on next page

SECURITY

Setting permissions for a role (continued)

STEP

ACTION

3

Review the permissions, and de-select ☐ those permissions that the Team Member role should not have. Select ☒ those permissions that Team Members should have.

NOTE: If outside parties, such as vendors, are going to be added to the project, set the Team Member permissions to **View** only those items an outside party can have access to, and de-select all other permissions. **All participants to a project automatically belong to the Team Member role.** Set the vendor role to the same minimal permissions.

You can add additional permissions to individuals or other roles as needed.

Click the **Submit** button.

On the **Setup** window, click **Security** again.

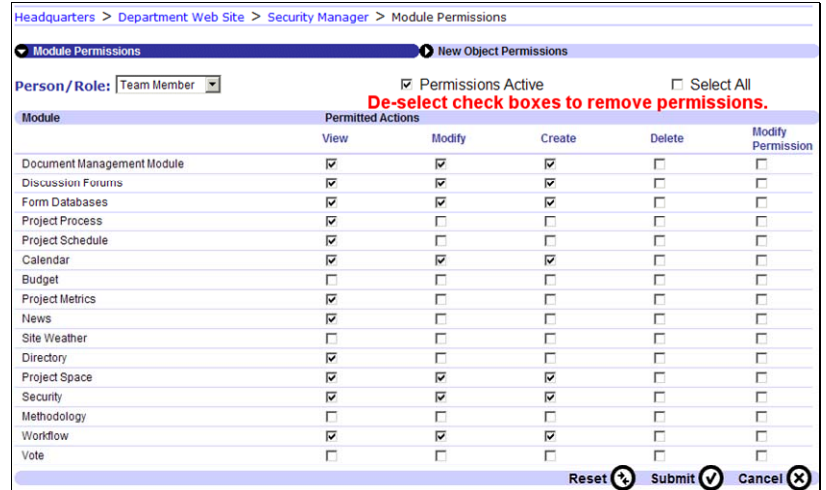
4

Click the **New Object Permissions** tab.

The **New Object** window appears.

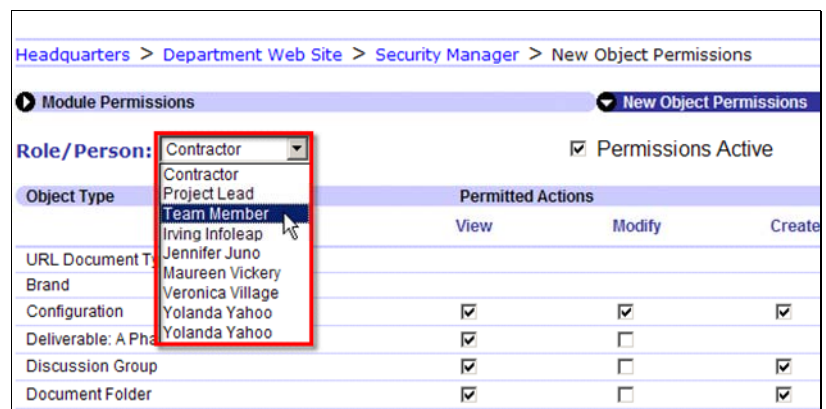
5

Select the role from the **Person/Role** drop-down list.



Module	View	Modify	Create	Delete	Modify Permission
Document Management Module	☒	☒	☒	☐	☐
Discussion Forums	☒	☒	☒	☐	☐
Form Databases	☒	☒	☒	☐	☐
Project Process	☒	☐	☐	☐	☐
Project Schedule	☒	☐	☐	☐	☐
Calendar	☒	☒	☒	☐	☐
Budget	☐	☐	☐	☐	☐
Project Metrics	☒	☐	☐	☐	☐
News	☒	☐	☐	☐	☐
Site Weather	☐	☐	☐	☐	☐
Directory	☒	☐	☐	☐	☐
Project Space	☒	☒	☒	☐	☐
Security	☒	☒	☒	☐	☐
Methodology	☐	☐	☐	☐	☐
Workflow	☒	☒	☒	☐	☐
Vote	☐	☐	☐	☐	☐

New Object Permissions



Object Type	View	Modify	Create
URL Document T			
Brand			
Configuration	☒	☒	☒
Deliverable: A Pha	☒	☐	
Discussion Group	☒	☐	☒
Document Folder	☒	☐	☒

Continued on next page

Setting permissions for a role (continued)

STEP

ACTION

6

Review the permissions, and de-select ☐ those permissions that the selected role should not have. Select ☒ those permissions that the role should have.

Click the **Submit** button to return to the Setup window.

Headquarters > Department Web Site > Security Manager > New Object Permissions

Module Permissions New Object Permissions

Role/Person: Team Member ☒ Permissions Active ☐ Select All

Object Type	Permitted Actions				
	View	Modify	Create	Delete	Modify Permission
URL Document Type					
Brand	☐	☐	☐	☐	☐
Configuration	☐	☐	☐	☐	☐
Deliverable: A Phase Deliverable	☒	☐	☐	☐	☐
Discussion Group	☒	☐	☒	☐	☐
Document Folder	☒	☒	☒	☐	☐
Document	☒	☒	☐	☐	☐
Calendar Event	☒	☐	☐	☐	☐
Form Type	☒	☐	☐	☐	☐
Form instance data (all versions)	☒	☒	☒	☐	☐
Gate: A Phase Gate	☒	☐	☐	☐	☐
Security Group	☒	☐	☐	☐	☐
Calendar Meeting	☒	☐	☐	☐	☐
News	☒	☐	☐	☐	☐
Phase: A Process Phase	☒	☐	☐	☐	☐
Process: A Project Process	☒	☐	☐	☐	☐
Scheduled Subscription					
Subscription					
Schedule Task or Milestone	☒	☐	☐	☐	☐
Workflow	☒	☐	☐	☐	☐

Reset Cancel

EXAMPLE OF MODULE PERMISSIONS OVERRIDING OBJECT PERMISSIONS

If the Document Management Module *View* permission is deactivated for a person or role, then the person/role will not be able to view, modify, create, delete, or modify permissions of the Document Management Module ("Document Vault").

The **Modify** permission for the Document Vault means that the user can check out documents and change document properties. The **Create** permission for a Document Vault means that the user can add new documents, create folders, etc. See page 17 for descriptions of other modules and their associated objects.

When the *View* permission for a module is removed, the person/role will not be able to view, modify, create, delete, or modify the security of any **objects** (document folders or documents) associated with that module.

Module	Permitted Actions		
	View	Modify	Create
Document Management Module	☐	☒	☒

Object Type	Permitted Actions		
	View	Modify	Create
URL Document Type	Object Permissions are overridden by Module Permissions.		
Brand			
Configuration	☐	☐	☐
Deliverable: A Phase Deliverable	☒	☐	
Discussion Group	☒	☐	☒
Document Folder	☒	☐	☒
Document	☒	☐	
Calendar Event	☒	☐	

Exception: The user who originally uploaded a document will still be able to access this document (from links to other objects or from the "recently modified documents" channel) after this new security setting takes effect. The administrator can remove personal document permissions from the user by clicking the specific document and altering the security settings, but this action would have to be done for *each document the user created* before the new settings took effect.

SECURITY

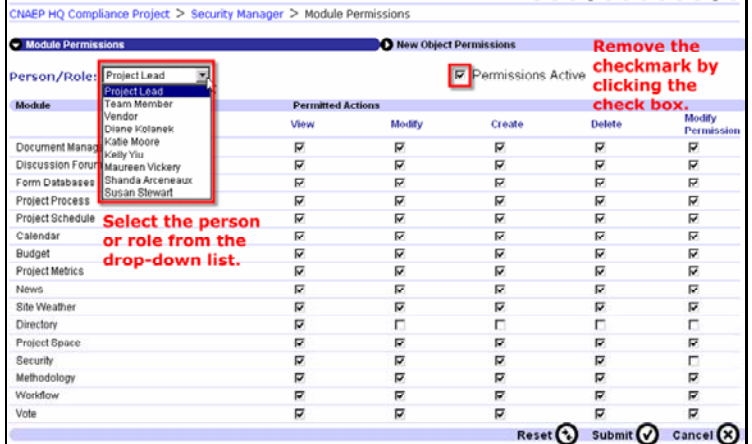
Permissions Active - deactivate all permissions simultaneously

It's possible to deactivate all Module Permissions or New Object Permissions at the same time for a role or person. This is achieved by de-selecting ☐ the **Permissions Active** check box.

- When the Permissions Active check box is checked ☒ (default setting), the permitted actions are available to be assigned for the current person or role.
- When the Permissions Active check box is blank ☐, all permitted actions are simultaneously deactivated for that role or person. (This is not readily apparent since the check box settings under the **Permitted Actions** columns will not change.)

TO SIMULTANEOUSLY DEACTIVATE ALL PERMISSIONS

STEP	ACTION
1	Each tab in the Security Manager has a Permissions Active check box. This allows the space administrator to remove permissions to all modules or all new objects from either a Person or a Role. To deactivate all permissions for a Person or a Role, select the Person/Role from the Person/Role drop-down list, and then deselect ☐ the Permissions Active check box.
2	Click the Submit button to save your changes.



Roles include Space Administrator, Team Member, and other roles created in the Team Directory. **Person** refers to the participants' individual names.

New Object Settings are not Retroactive!

- Changes to New Object Permission settings do not affect previously created objects. Changes will only apply to new objects that are created in the future. So, if a team member adds a document to the Document Vault, and the space administrator later changes the New Object Permission for Documents, the team member's access to existing documents in the Document Vault will be unaffected. Items added prior to the changed in security must be secured individually by selecting the object, and then clicking the security  icon.
- Changes to Module permissions limit the users' access to all objects within the module **regardless** of whether those objects were created before or after the changed module permission. The only exception is objects that a user created can still be accessed by that user through links and channels outside the module. This access can also be revoked by the Space Administrator, but must be done individually for each object using the Security  button on the toolbar. For

SECURITY

example, the user who originally uploaded a document will still be able to access this document (from links to other objects or from the “recently modified documents” channel) after this new security setting takes effect. The administrator can remove personal document permissions from the user by clicking the specific document and altering the security settings, but this action would have to be done for *each document the user created* before the new settings took effect.

A solid blue horizontal bar spanning the width of the page content area.

Understanding the “Permissions Active” Checkbox

A ROLE’S MODULE PERMISSIONS

When the Permissions Active check box under Modules is checked for a Role:

- Any person belonging to that role will be granted the module permissions checked for that role in addition to permissions granted to that person through other roles. Permissions granted by roles are additive.
- An individual person’s permissions will override any role permissions for the module.

When the Permissions Active check box under Modules is unchecked for a Role:

- Any person belonging to that role will no longer have permissions the modules granted by that role. However, if a person belongs to a role besides the deactivated role, the permissions granted for the other role will still apply. Permissions granted by roles are additive.
- An individual person’s permissions will override any role permissions for the module.

A PERSON’S MODULE PERMISSIONS

When the Permissions Active check box under Modules is checked for a Person:

- The person will only be granted the module permissions selected for them as a person.
- All module permissions assigned through other roles (the person belongs to) will be overridden.
- The person module permission should not be used unless absolutely necessary to limit a specific person’s access.

When the Permissions Active check box under Modules is unchecked for a Person:

- All module permissions for that person will be determined only by the roles they are a member of.

A ROLE’S NEW OBJECT PERMISSIONS

When the Permissions Active check box under New Object Permissions is checked for a Role

- Any person belonging to that role will be given the selected access permissions to newly created objects in the workspace via that particular role. These new object permissions are in addition to any other new object permissions granted by other roles.
- Changes to new object permissions do not affect previously-created objects.

When the Permissions Active check box under New Object Permissions is unchecked for a Role

- Any person belonging to that role will not be given access to any newly created objects in the workspace via that particular role. However, if a person belongs to other roles, the New Object permissions granted for the other roles will still apply.
- Changes to new object permissions do not affect previously-created objects.

A PERSON’S NEW OBJECT PERMISSIONS

When the Permissions Active check box under New Object Permissions is checked for a Person:

- A person’s permissions to newly created objects will be determined solely by the new object permissions granted this person’s permissions.

SECURITY

- All other new object permissions granted by roles the person is a member of will be overridden.
- The person new object permissions should not be used unless absolutely necessary to limit a specific person's access to objects.
- The person's access to previously-created objects will not be affected.

When the Permissions Active check box under New Object Permissions is unchecked for a Person:

- A person's permissions to newly created objects will be determined solely by the new object permissions granted to roles they are a member of.
- The person's access to previously-created objects will not be affected.

Discussion Forums – no security settings apply

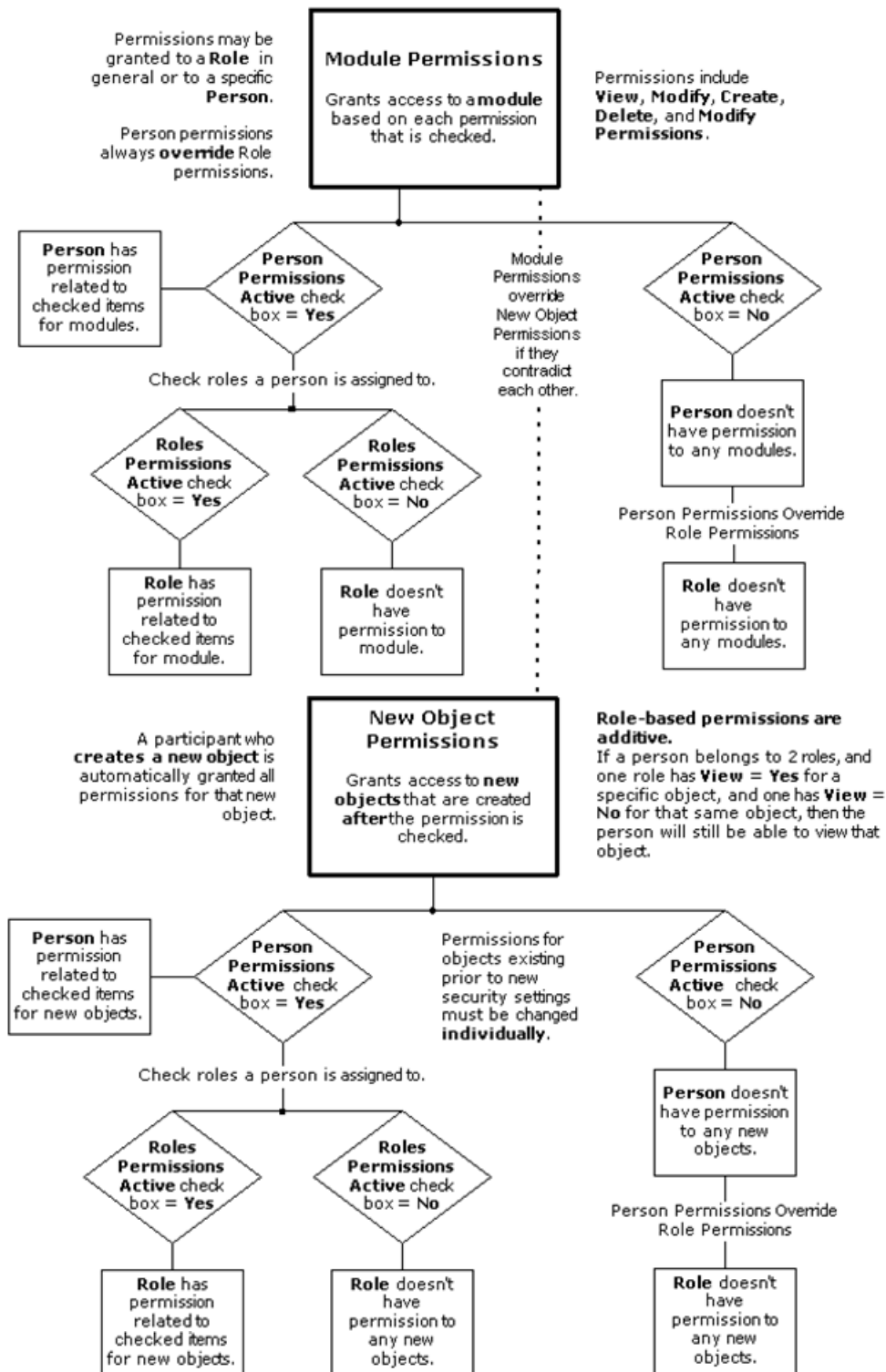
At this time, security access to the Discussion Forums can only be controlled at the module level. If a person or role is given access to the Discussions module, they will have access to all discussion groups. It is not currently possible to provide access to specific discussion groups. Any team member of the workspace has access to read all the discussions.

Review: The Difference between Module and New Object Permissions

- **Module permissions** affect a Role or a Person's ability to enter a module and view, modify, create, delete objects in a particular module. For example, if a person does not have view permission for the Document module, they can not even enter that module to see a listing of documents. If a person have view access but not create access for the Document module, they can enter the document module, see listings of documents, view document contents, but they cannot create a new document or folder.
- **New Object Permissions** determine the default permissions that will be given to an object when it is created. Changes to New Object permissions are not retroactive to previously created objects.
- **Object permissions are set from the tool bar for individual objects and** determine a role's or person's ability to view, modify, create, delete, or modify permissions for objects such as documents, forms, folders, and calendar events.
- **Module** permissions override **Object** permissions.
- **Person** permissions override **Role** permissions.
- The creator of an object **always has all permissions** granted for that object, unless permissions are specifically removed by the Space Administrator.

Hierarchy for the Permissions Active check box

SECURITY



Description of Modules and Objects

MODULE & ASSOCIATED OBJECTS	DESCRIPTION
Calendar	For scheduling tasks, meetings, and events

Calendar Event

Calendar Meeting

Directory	Lists team members who have accepted or been invited to the project.
Discussion Forums	Area to enter topics for discussion.
Discussion Group	Topics created in the discussion forum.
Document Management	Document vault used for storing files and URLs. Folder/subfolder configuration.
Document	File or URL uploaded in the document vault
Document Folder	Folders created to organize documents.
Form Databases	Data entered into a form template created in the Form Designer.
Form Instance Data	Data entered in a form field.
Form Type	A field or list created in the Form Designer.
Methodology	Lifecycle or Work Processes
Phase: A Process Phase	Used to break up a project into sets of tasks.
News	A bulletin board for recording items of interest to the team.
News Item	A news item that will be copied to the personal workspace dashboard of all participants.
Project Process	Lifecycle of the project. Where tasks and deliverables are defined.
Process: A Project Process	Each process only has one. The definition of the project.
Project Schedule (workplan)	The detailed project plan.
Schedule Task or Milestone	What needs to be done to complete the project.
Deliverable: A Phase Deliverable	A tangible outcome produced by the project.
Project Space (workspace)	The modules, channel bars, tabs, navigation bar, tabs, and action toolbar.
Configuration	The look and feel of the workspace.
Security (modify permissions)	Used to set permissions and access throughout the project.
Security Group	
Workflow (workflow designer)	Used to create an authorization or approval path for a document or form. Sends an electronic "envelope" to a participant's inbox.
Workflow	A workflow created in the Workflow Designer.

Team Members – Setting Security

Setting Object Permissions

The ability for team members to set permissions for individual objects (such as folders, documents, or forms) is determined by the permissions granted in the New Objects Permissions by the Space Administrator.

Team members can modify security for the objects they authored by clicking the **Security**  button (when it is active) in the action toolbar.

EXAMPLE: SETTING OBJECT PERMISSIONS FOR A DOCUMENT

STEP

ACTION

1

From the Document Vault window, click the radio button next to the object, and then click the **Security** button in the action bar.

The **Edit Role Entry** pop-up window appears.

2

To add or remove participants to/from the Permitted Actions, click the **People** tab.

The names of the participants are displayed.

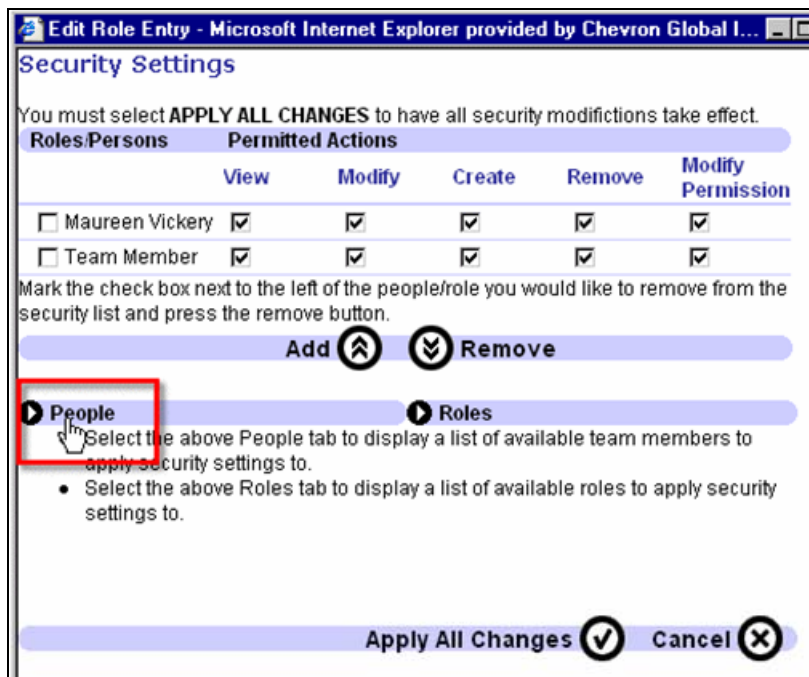


Chevron Project.Net Pilot > Project.net - Help Desk & Bugs Documentation > Document Vault

Click the radio button, and then click the Security button.

Contents of: [Top folder](#)

Name	Format	Ver	C/O	Status	Author	Last Modified	Size
Email	Folder						
Training Documents	Folder						
CPDEP website	URL				Complete Maureen Vickery	Jan 07, 2002	



Edit Role Entry - Microsoft Internet Explorer provided by Chevron Global I...

Security Settings

You must select **APPLY ALL CHANGES** to have all security modifications take effect.

Roles/Persons	View	Modify	Create	Remove	Modify Permission
☐ Maureen Vickery	☒	☒	☒	☒	☒
☐ Team Member	☒	☒	☒	☒	☒

Mark the check box next to the left of the people/role you would like to remove from the security list and press the remove button.

Add **Remove**

People **Roles**

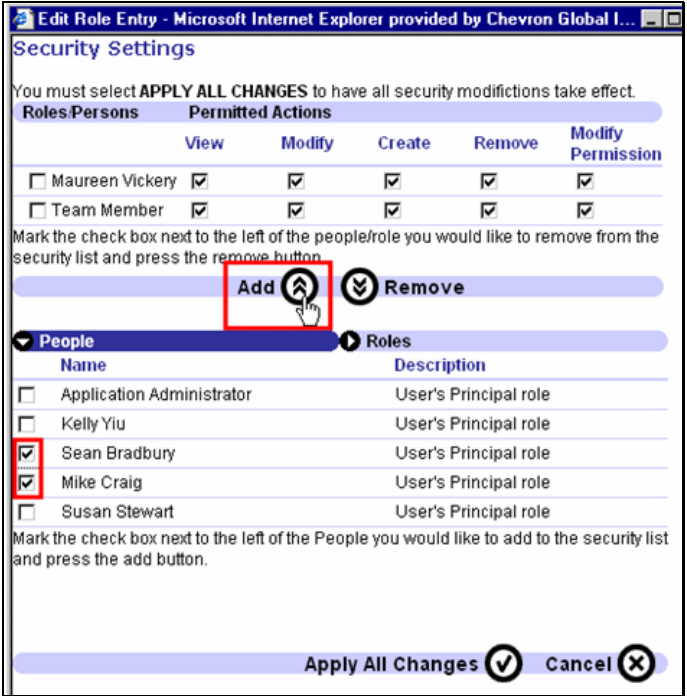
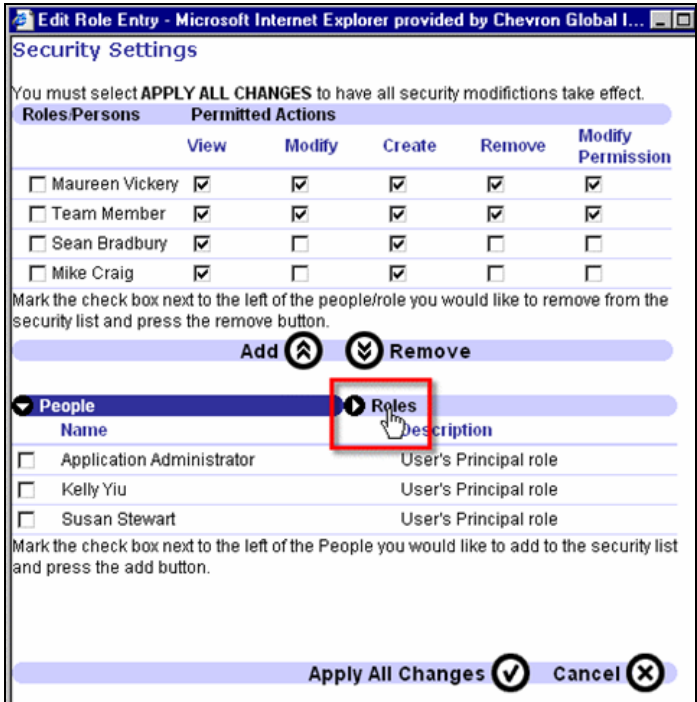
Select the above People tab to display a list of available team members to apply security settings to.

- Select the above Roles tab to display a list of available roles to apply security settings to.

Apply All Changes **Cancel**

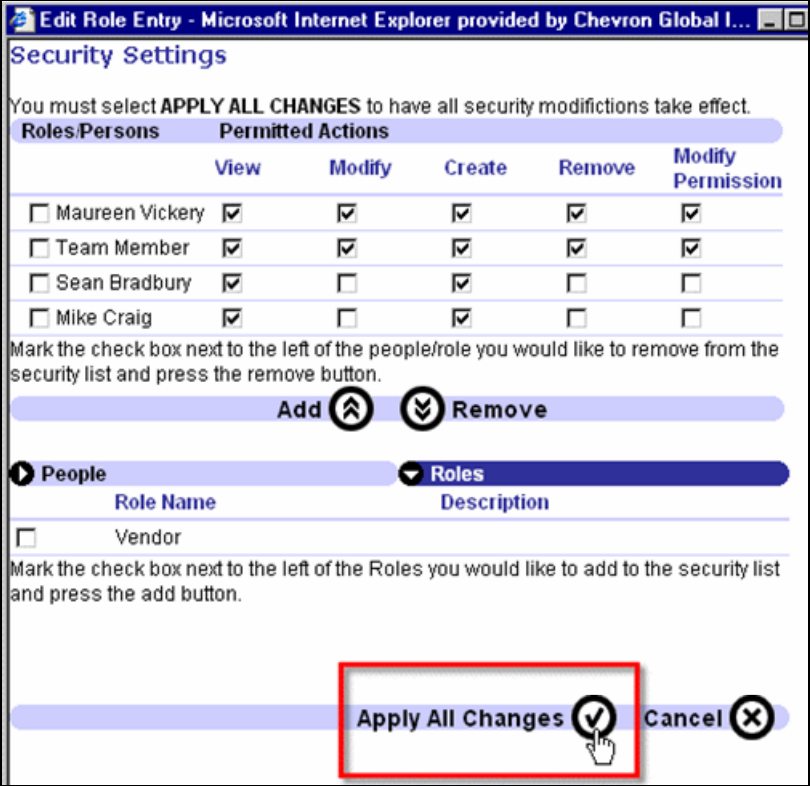
Continued on next page

Setting Object Permissions (continued)

STEP	ACTION
3	Select ☒ the check boxes from the People list to add participants, and then click the Add button. NOTE: To remove participants from the Permitted Actions list, select ☒ their check boxes, and then click the Remove button.
	 The screenshot shows the 'Edit Role Entry' window with the 'Permitted Actions' tab selected. The 'Add' button is highlighted with a red box. The 'People' list is visible below, with 'Sean Bradbury' and 'Mike Craig' selected.
4	When you are finished with the settings, click the Apply All Changes button. If you wish to change the roles assigned to permitted actions, then click the Roles tab. NOTE: In this example, Sean and Mike do not have permission to modify this object, although as team members they ARE assigned the permission to modify objects like this. In this case, the individual permission would OVERRIDE the team member permission. Therefore, Sean and Mike can't modify this particular object. TIP: Only modify an individual's permissions to a specific object if the individual doesn't already have permissions through an assigned role.
	 The screenshot shows the 'Edit Role Entry' window with the 'Roles' tab selected. The 'Roles' tab is highlighted with a red box. The 'People' list is visible below, with 'Sean Bradbury' and 'Mike Craig' selected.

Continued on next page

Setting Object Permissions (continued)

STEP	ACTION
5 Select ☒ the check boxes from the Roles list for the roles to add, and then click the Add button. In this example, we decided not to add any roles to the Permitted Actions. NOTE: To remove participants from the Permitted Actions list, select ☒ their check boxes, and then click the Remove button.	
6 Click the Apply All Changes button. The pop-up window automatically closes.	